



LYNX L-510



Web Interface User's Guide

ADSL2/2+ Ready Wireless LAN 802.11g 4 Port Ethernet & USB Combo Router

Contents

1. INTRODUCTION	4
1.1 FEATURES	4
2. YOUR GATEWAY AT A GLANCE.....	6
2.1 PORTS AND BUTTONS	6
2.2 LED DESCRIPTION	6
3. INSTALLING YOUR WIRELESS GATEWAY	7
4. SETTING UP YOUR WIRELESS GATEWAY (BASIC MODE).....	8
4.1 LOG INTO YOUR WIRELESS GATEWAY	8
4.2 QUICK START	9
4.3 DIAGNOSTICS TEST.....	11
4.3.1 <i>Ping Test</i>	12
4.4 REMOTE ACCESS.....	12
4.5 STATISTICS.....	13
4.6 WIRELESS	13
4.6.1 <i>Wireless Setup</i>	13
4.6.2 <i>Wireless Security</i>	15
4.7 SAVE SETTINGS.....	15
5. ADVANCED	17
5.1 LAN CONNECTION	17
5.1.1 <i>DHCP Configuration</i>	17
5.1.2 <i>Management IP (Changing the Wireless Gateway IP address)</i>	19
5.2 WAN CONNECTION.....	20
5.2.1 <i>Status</i>	20
5.2.2 <i>Configuring the WAN</i>	20
5.2.3 <i>New Connection</i>	21
5.2.4 <i>Modify an Existing Connection</i>	27
5.2.5 <i>Modem setup</i>	27
5.2.6 <i>Firewall/NAT Services</i>	28
5.2.7 <i>UPnP</i>	28
5.2.8 <i>Modem Status</i>	28
5.3 ROUTES	29
5.3.1 <i>Show Routes</i>	29
5.3.2 <i>Static Routing</i>	29
5.3.3 <i>Dynamic Routing</i>	30
5.4 SECURITY.....	31
5.4.1 <i>Port Forwarding</i>	31
5.4.2 <i>Access Control</i>	32
5.4.3 <i>IP Filter</i>	33
5.4.4 <i>DMZ</i>	34
5.4.5 <i>MAC Filter</i>	35
5.4.6 <i>LAN clients</i>	36
5.5 APPLICATIONS	37

5.5.1	<i>Dynamic DNS</i>	37
5.5.2	<i>System Time</i>	37
5.5.3	<i>DNS Proxy Settings</i>	38
5.6	WIRELESS	39
5.6.1	<i>Wireless Security (Advance)</i>	39
5.6.2	<i>Wireless Management</i>	40
5.6.3	<i>User Management</i>	41
6.	APPENDIX A: TROUBLESHOOTING	45
6.1	THE WIRELESS GATEWAY IS NOT FUNCTIONAL.....	45
6.2	I CAN'T CONNECT TO THE WIRELESS GATEWAY.....	45
6.3	THE DSL LINK LED CONTINUES TO BLINK BUT DOES NOT GO SOLID	45
6.4	THE DSL LINK LED IS ALWAYS OFF	46
7.	WIRELESS GATEWAY TERMS	47

1. Introduction

The ADSL 2/2+ Ready Wireless LAN 802.11g 4 Port Ethernet & USB Combo 4 Port Router is the perfect high-speed WAN bridge/router.

This full-featured product is specifically designed allow maximum of 4 Ethernet-workstations to be connected to the Internet and directly connect to your local area network via high speed 10/100 Mbps Ethernet. Most importantly users using wireless workstations will be able to connect to the Internet using 802.11g wireless technology. The Wireless Gateway has also full NAT firewall and DMZ services to block unwanted users from accessing your network.

For game users, the Wireless Gateway had already pre configured for several low latency game ports. Just click on the game you are playing on line and the rest is done for you

The Wireless Gateway is fully compatible with all PCs; as long as the PC supports an Ethernet interface and is running a TCP/IP protocol stack, your PC can have high-speed WAN access. So, plug in the Wireless Gateway (refer to easy start guide), configure it (per your ISP's requirements) and enjoy the fast Internet access like never before. This router also provides future proof functionality with higher data transmission rates with ADSL2,ADSL2+, Extended Reach-ADSL support.

1.1 Features

ADSL/ATM Support

- ANSI T1.413 issue 2, ITU-T G.992.1 (G.dmt) and G.992.2 (G.lite) compliant
- ADSL2, ADSL2+, RE-ADSL compliant
- Rate Adaptive modem at 32 Kbps steps
- Dynamic Adaptive Equalisation to improve Carrier's service area
- Bridge Tap Mitigation support
- ATM Layer with Traffic shaping QoS Support (UBR, CBR, VBR-rt, VBR-nrt)
- AAL ATM Attributes - AAL5
- Multiple PVC up to 8 support (Bridge Support)
- Spectral compatibility with POTS
- F5 OAM Loopback/Send and Receive

Encapsulation Support

- RFC2684 Bridge and Routed LLC and VC Mux support
- RFC2364 PPPoA Client support
- RFC2516 PPPoE Client support
- RFC2225/RFC1577 Classical IP Support
- Transparent Bridge Support
- PAP/CHAP/MS-CHAP for Password Authentication Support

Network Support

- Static IP, Dynamic RIP routing support
- IP/TCP/UDP/ICMP/ARP/RARP Application Support
- Network Address Translation (NAT)
- Port Mapping/Forwarding
- Easy setup of Port Forwarding rules for popular Games/Application
- NAT Application Level Gateway for popular applications
- DHCP Server/Relay/client
- DNS Relay Agent
- DMZ support
- Single Session IP Sec and PPTP/L2TP VPN pass through support

-
- PPP Always on with configurable timeout
 - PPP Dial on Demand
 - Universal Plug and Play Support

WLAN Support

- IEEE 802.11, 802.11B and 802.11G compliant
- Conforms to Wireless Ethernet Compatibility Alliance (WECA) Wireless Fidelity (Wi-Fi tm) standard
- Supports 802.11b and 802.11g simultaneously
- Support Direct Sequence Spread Spectrum (DSSS) technology
- Operating Range of >300 Meters (Open Air)

Management Support

- Web Based HTTP management GUI
- TFTP/FTP Support for Firmware Upgrade
- Web Based Firmware Upgrade (Local)
- Soft Factory Reset Button via Web GUI
- Diagnostic Test (DSL, OAM, Network, Ping Test)
- Telnet/CLI (Read Only)
- Syslog Support
- Firmware upgrade-able for future feature enhancement

Security Support

- NAT for basic Firewall support
- Packet Filtering Firewall Support
- Stateful Packet Inspection Support
- Protection against Denial of Service attacks
- Password Authentication to Modem

External Connectors:

- 1 x RJ-11 Telephone socket for ADSL line
- 4 x RJ45 for 10/100Base-T Ethernet (MDI-X)
- 1 x USB 1.1 Type B
- 1 x DC Jack for Power Input
- 1 x Factory Default Reset Button
- 1 x On/Off Power Switch
- 1 x Co-axial Connector for Detachable 180 degree Rotate-able 2.4Ghz 3 dBi Antenna

Platform Support:

- Windows 98SE
- Windows ME
- Windows 2000
- Windows XP
- Windows 2003

2. Your gateway at a glance

The ADSL Ethernet & USB Combo may have different ports and LEDs. Let's take a look at the different options. Depending upon your model, it may have some or all of the features listed below

2.1 Ports and buttons

Reset and Restore to Factory Defaults: The restore to factory defaults feature will set the Wireless Gateway to its factory default configuration by resetting the Wireless Gateway. You may need to place the Wireless Gateway into its factory defaults if the configuration is changed, you lose the ability to interface to the Wireless Gateway via the web interface, or following a software upgrade. To reset the Wireless Gateway, simply press the reset button for about ~ 10 seconds. The Wireless Gateway will be reset to its factory defaults and after about 30 ~ 40 seconds the Wireless Gateway will become operational again.

LAN (local area network) E1 to E4 port(s): connect to Ethernet network devices, such as a PC, hub, switch, or routers. Some Wireless Gateway came with a single LAN connection and some come with four LAN connections. Depending on the connection, you may need a cross over cable or a straight through cable.

Power is where you connect the power. Make sure to observe the proper power requirements. The required power is 9 volts.

USB (universal serial port): connects to a PC's USB port. The Wireless Gateway only supports Window's based PCs via an RNDIS driver (included in the software).

DSL port: This is the WAN interface that connects directly to your phone line.

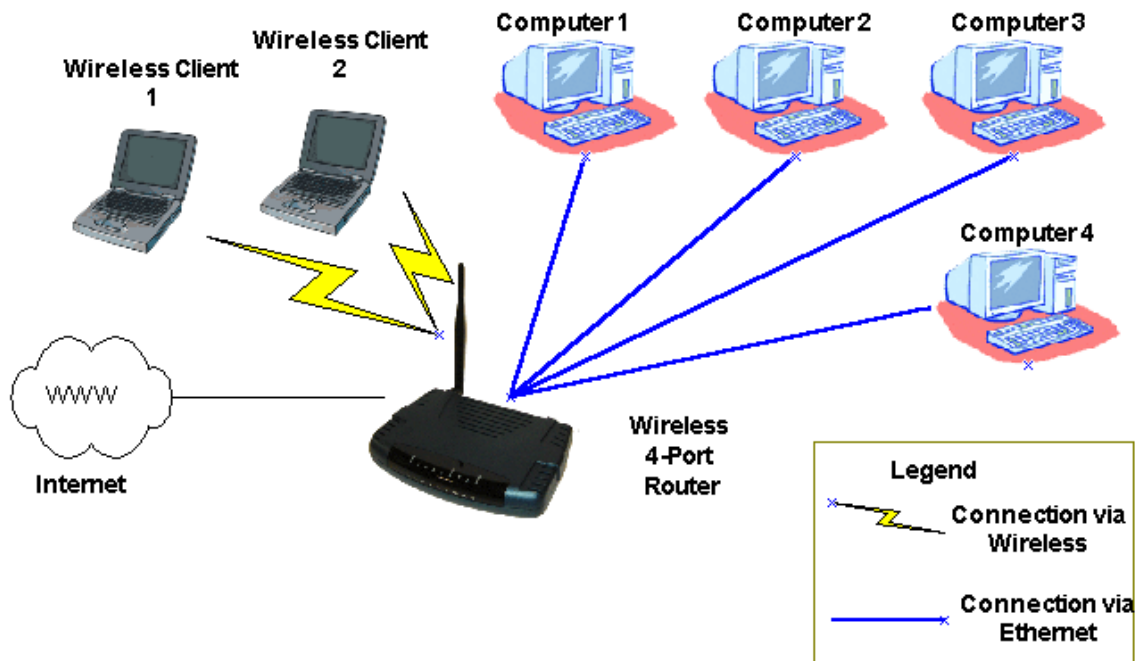
2.2 LED description

1. **POWER**
Lights up when power is supplied to the Wireless Gateway.
2. **(E1- E4)**
Lights up when the Ethernet cable is properly connected from your Wireless Gateway to the Ethernet Card.
Flickers when the ADSL is transmitting/receiving data.
3. **WIRELESS**
Lights up when after the router's wireless feature is activated.
Flickers when the ADSL is transmitting/receiving data to a connected wireless client.
4. **USB**
Lights up when the USB connection is established.
Flickers when the ADSL is transmitting/receiving data
5. **DSL**
Lights up when the DSL connection is established.
Flickers when the Wireless Gateway is trying to establish a connection with the ADSL Service Provider.
6. **INTERNET**
Lights up when the PPP connection is established.

3. Installing your Wireless Gateway

1. Locate an optimum location for the Wireless Gateway.
2. For connections to the Ethernet and DSL interfaces, please refer to the **easy start guide**.
3. Connect the AC Power Adapter. Depending upon the type of network, you may want to put the power supply on an uninterruptible supply. Only use the power adapter supplied with the Wireless Gateway. A different adapter may damage the product.

Now that the hardware installation is complete, proceed to **Chapter 4: Setting up your Wireless Gateway**



4. Setting up your Wireless Gateway (Basic Mode)

Basic tabs consist features which are catered for basic users.

This section will guide you through your Wireless Gateway's configuration. The Wireless Gateway is shipped with a standard PPP configuration.

4.1 Log into your Wireless Gateway

To configure your Wireless Gateway, open your web browser. You may get an error message at this point; this is normal. Do not panic!. Continue following these directions. Type the default IP address (**192.168.1.1**) or type the short-cut name **login.router**. Press the **Enter** key and the following screen.

Note: Before setting up your Wireless Gateway, make sure you have followed the easy start guide. You should have your computers configured for DHCP mode and have proxies disabled on your browser. Also if you access the Wireless Gateway, and instead of getting a login screen, the browser instead displays a login redirection screen, you should check your browser's setting, and verify that JavaScript support is enabled. Also, if you do not get the screen shown in Figure 1, you may need to delete your temporary Internet files (basically flush the cached web pages).

Upon entering the default IP address or the short-cut name (**login.router**), if the user is first time login, the user will be brought to the "Setup Wizard" page. As show in figure 1.1

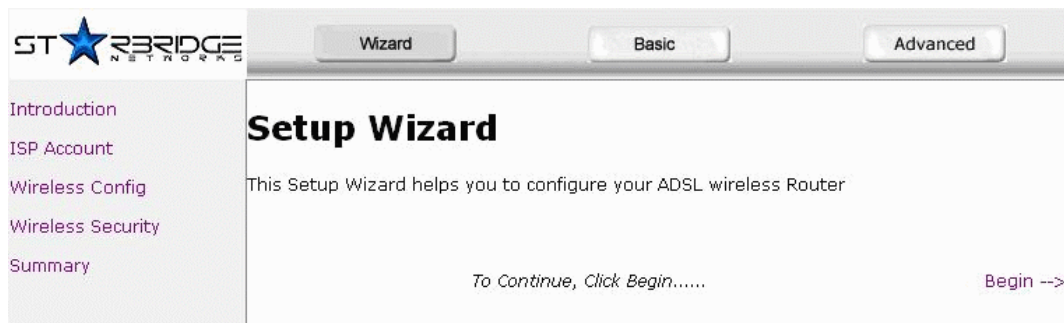


Figure 1.1 (Setup Wizard Screen)

If the your are not login-in the first time, the router will direct you to the "Home Page" as shown in figure 1.2

Wizard

Basic

Advanced

[Home](#)
[Quick Start](#)
[Diagnostic](#)
[Statistics](#)
WIRELESS
[Wireless Setup](#)
[Wireless Security](#)
[Restart Router](#)
[Save Settings](#)

Home Page

Connection Information

DSL	Up
Downstream/Upstream(Kbps)	0/0
Internet	Not Connected
User ID	username
IP Address	N/A
Default Gateway	N/A
DNS	Auto

RestartConnect

Router Information

Model	Lynx 510 4-Port Wireless Router
Serial Number	none
Firmware Version	43.48.2
Ethernet MAC address	00:30:0A:1E:75:2D
DSL MAC address	00:30:0A:1E:75:2F
USB MAC address	00:30:0A:1E:75:2E
NAT	Enabled
Firewall	Disabled

Local Network

LAN IP Address	192.168.1.1
DHCP	Enabled
DHCP Range	192.168.1.10 - 192.168.1.200
Ethernet	Connected
USB	Disconnected

Figure 1.2 (Setup Wizard Screen)

4.2 Quick Start

This screen appears will the user clicks on the Quick Start hyperlink.

The screen as shown in Figure 2.1 will be shown when the router detected that there is no DSL line connected to the modem. Please follow the hint to rectify the problem.

Hint : Your DSL link is down.

1. Please check if your DSL line is connected to your modem.

2. Please wait for the DSL link to establish if your DSL cable is connected. You will be redirected when the DSL link is up.

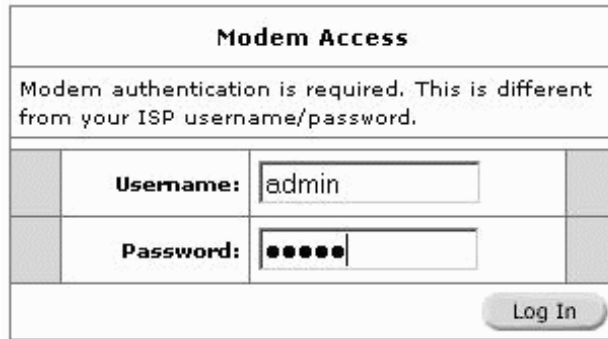
Figure 2.1 (Quick Start Error page)

By default the Wireless Gateway has being configured to PPP connection and user would only need to enter the username and password (as specified by the local ISP) to make connection to the Internet.

The Quick Start page is meant for basic users whom only require easy and seamless connectivity to the Internet without worrying about any other advance configuration setting. If you are in doubt for what content to enter for the Protocol, VPI and VCI, please contact your Service Provider for details.

Important:

After clicking on Connect, please be sure to “Save Settings” to register the username / password or any other changes.



The image shows a web form titled "Modem Access". Below the title, it states "Modem authentication is required. This is different from your ISP username/password." There are two input fields: "Username:" with the text "admin" and "Password:" with masked characters "•••••". A "Log In" button is located at the bottom right of the form.

Figure 2.2 (Quick Start page)

Upon clicking on “Connect” button the status will be shown as below.



The image shows a status page titled "Try to connect to ISP". The main content area displays the text "Trying to Connect to ISP" in a monospaced font.

Figure 2.3 (Quick Start Connection status page)

The router will check for wrong username and password, if the Internet connection could not be established. You can click on “here” hyperlink to re-enter your username and password.



The image shows an error message box titled "Connect to Internet Fail". The main text reads "Connection to the Internet cannot be established". Below this, it says "Tips: Please check your username and password." and "Please click OK to continue." There is an "OK" button at the bottom left.

Figure 2.4 (Quick Start Connection Fail page)

4.3 Diagnostics Test

Diagnostic Test is used for investigating whether the Wireless Gateway is properly connected to the WAN Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link;

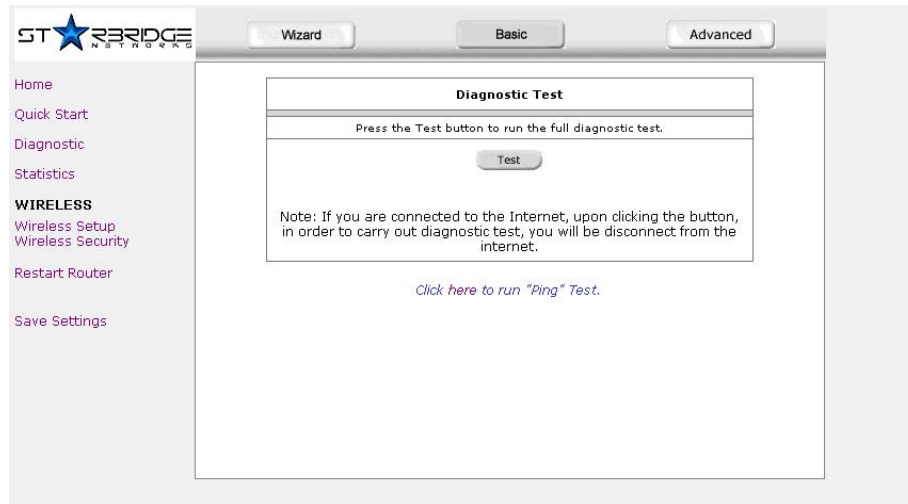


Figure 3.1 (Diagnostic Test screen)

After running the Diagnostic Test, the screen will indicate that the portion which pass or fail the test. Please click on the **Help** links, which will provide remedy to the problem as shown in (Figure 3.2). The purpose of the "Fix It " button is to restore the router's VPI and VCI to its originated setting.

Diagnostic		
Interface (PC to Modem)	PASS	HELP
Modem	PASS	HELP
Modem to ADSL line connection	FAIL	HELP

Fix It!

Click here to run "Ping" Test.

Figure 3.2 (Diagnostic Test Result screen)

4.3.1 Ping Test

Once you have your Wireless Gateway configured, it is a good idea to make sure you can ping the network. You can get to the Ping page by clicking on the “**here**” hyperlink in Diagnostic Page. Type the target address that you want to ping. If you have your PC connected to the Wireless Gateway via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. If your ISP has provided their server address you can try to ping the address. If the pings for both the WAN and the LAN side complete, and you have the proper protocols configured, you should be able to surf the Internet.

By default when you select ping test, the Wireless Gateway will ping itself 3 times. As shown in Figure 20, the Wireless Gateway passed the Ping test; this basically means that the TCP/IP protocol is up and running. If this first Ping test does not pass, the TCP/IP protocol is not loaded for some reason; you should restart the Wireless Gateway.

The screenshot shows a web interface titled "Ping Test". It contains three input fields: "Enter IP Address to ping:" with the value "192.168.1.1", "Packet size:" with the value "64" and the unit "bytes", and "Number of echo requests:" with the value "3". A "Test" button is located to the right of these fields. Below the input fields is a text area displaying the results of the ping test:

```
PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255
time=0.0 ms
--- 192.168.1.1 ping statistics ---
```

Figure 3.3 (Ping Test screen)

4.4 Remote Access

Note: Remote Access Hyperlink will only be visible to you, if you have successfully connected to the Internet.

Remote Access will allow a remote party to access your router, if you enable Remote Access and enter the remote party's IP address.

Remote Access	
Enable Remote Access	☒ Yes ☐ No
Remote IP Address:	203.126.99.251 Netmask: 255.255.255.0
Note: Enter IP Address of you distant party.	
WAN IP Address: 203.125.77.220	
Warning: By enabling Remote Access, it will allow remote user with a specific IP address to gain access to your router's web configuration by knowing your WAN IP	
Apply	

Figure 4 (Remote Access screen)

4.5 Statistics

Information regarding the Status and Statistics of your Ethernet, USB and DSL line will be displayed

Ethernet Network Statistics	
Choose an interface to view your network statistics:	
☒ Ethernet ☐ USB ☐ DSL	
Transmit	
Good Tx Frames	3593
Good Tx Broadcast Frames	1
Good Tx Multicast Frames	0
Tx Total Bytes	2340497
Collisions	0
Error Frames	0
Carrier Sense Errors	0
Receive	
Good Rx Frames	2926
Good Rx Broadcast Frames	2
Good Tx Multicast Frames	0
Rx Total Bytes	358731
CRC Errors	0
Undersized Frames	0
Overruns	0
Refresh	

Figure 5 (Statistics screen)

4.6 Wireless

4.6.1 Wireless Setup

The SSID default which is defaulted as "yournetworkname" can be changed.

SSID is wireless network name for the wireless router, your wireless client will need this name for wireless connection.

The wireless setup allows the user to enable or disable the AP (access point for the wireless feature). Disabling of A.P will prevent the wireless router from emitting any wireless signal. User can make change the Country selection, which is defaulted as US, channel 6.

After any changes to the Wireless Setup, please click on “Restart Access Point” to allow the Wireless features to apply the changes.

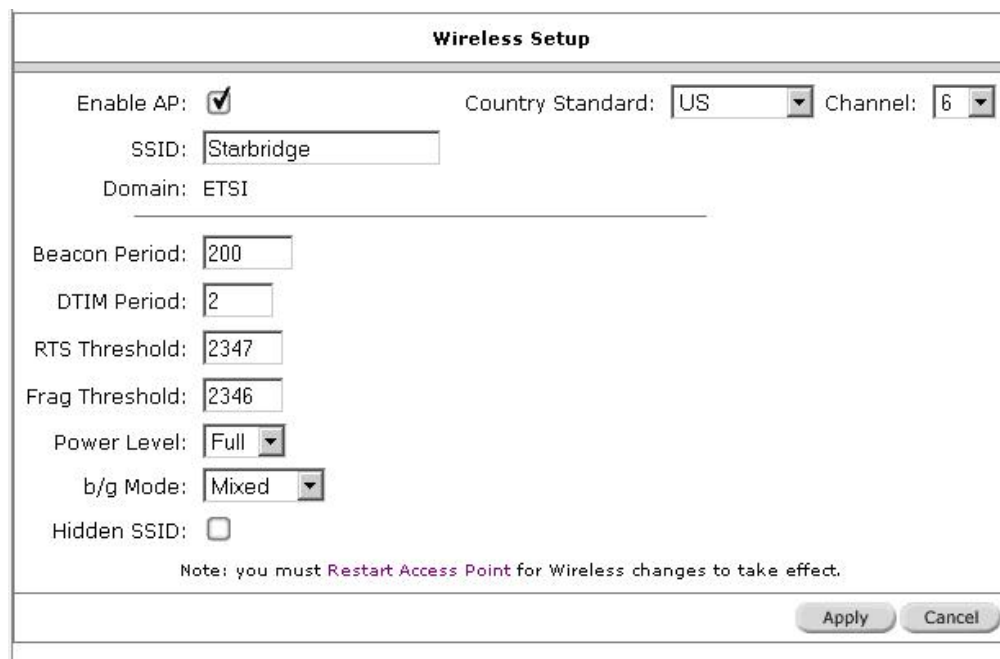


The screenshot shows the 'Wireless Setup' window with the following fields and controls:

- Enable AP:** ☒
- Country Standard:** US (dropdown menu)
- Channel:** 6 (dropdown menu)
- SSID:** Starbridge (text input field)
- Domain:** ETSI (text input field)
- Advanced:** A button to expand the configuration options.
- Note:** you must Restart Access Point for Wireless changes to take effect.
- Buttons:** Apply and Cancel at the bottom right.

Figure 6.1 (Wireless Setup screen)

For user who wants to explore the advanced feature, you can click on the Advance button. The options listed can be changed to cater for advance users.



The screenshot shows the 'Wireless Setup' window with the 'Advanced' section expanded, displaying the following fields and controls:

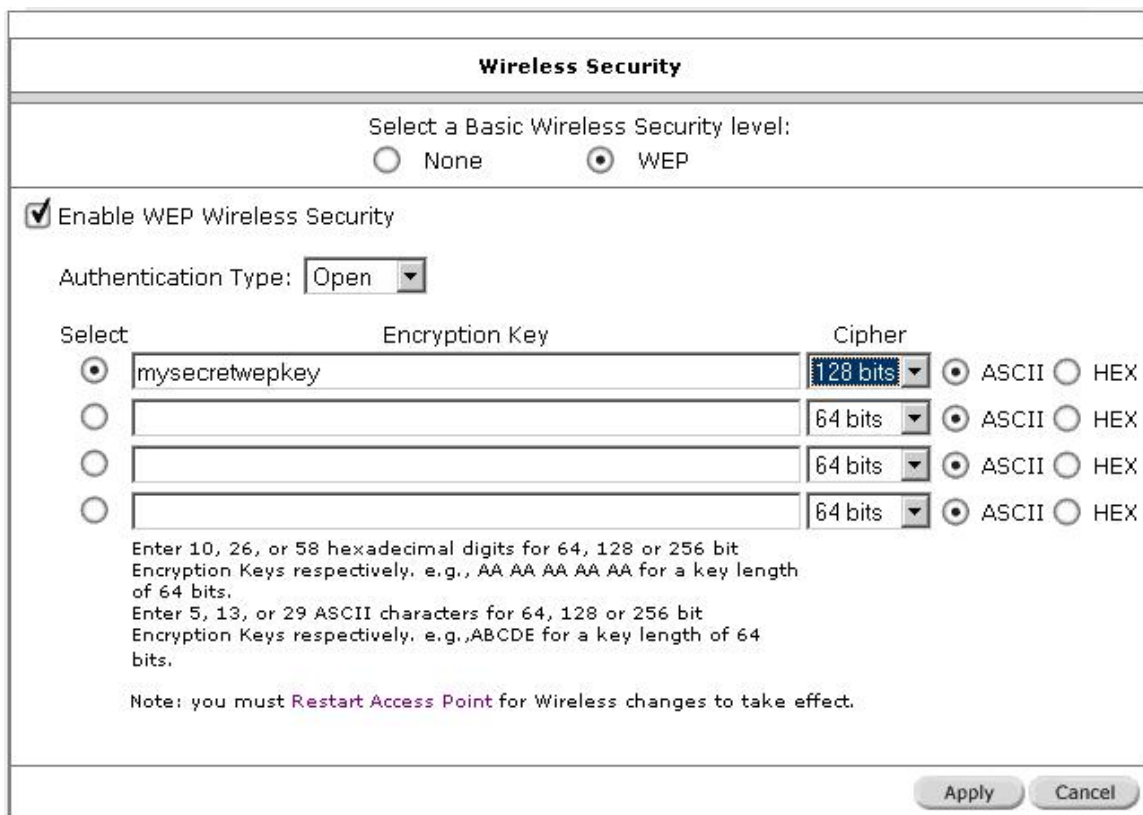
- Enable AP:** ☒
- Country Standard:** US (dropdown menu)
- Channel:** 6 (dropdown menu)
- SSID:** Starbridge (text input field)
- Domain:** ETSI (text input field)
- Beacon Period:** 200 (text input field)
- DTIM Period:** 2 (text input field)
- RTS Threshold:** 2347 (text input field)
- Frag Threshold:** 2346 (text input field)
- Power Level:** Full (dropdown menu)
- b/g Mode:** Mixed (dropdown menu)
- Hidden SSID:** ☐
- Note:** you must Restart Access Point for Wireless changes to take effect.
- Buttons:** Apply and Cancel at the bottom right.

Figure 6.2 (Wireless Setup screen)

4.6.2 Wireless Security

It is important for user to enforce security in wireless LAN environment, this is to prevent unauthorized wireless users from accessing your router. On default, no wireless security is configured, the “None” radio button is selected.

1. In order implement security, WEP option must be selected
2. Check on “Enable WEP Wireless Security” option
3. Select the “Cipher” option, the available options are 64bits, 128bits and 256 bits.
4. Select ASCII or HEX option
5. Follow the example as listed below to configure the wireless security settings.
6. You can configure up to 4 sets of keys for your wireless client.



The image shows a web-based configuration interface for wireless security. At the top, the title "Wireless Security" is centered. Below it, a section titled "Select a Basic Wireless Security level:" contains two radio buttons: "None" and "WEP". The "WEP" button is selected. Below this, a checkbox labeled "Enable WEP Wireless Security" is checked. Underneath, the "Authentication Type:" is set to "Open" in a dropdown menu. The main section is titled "Select Encryption Key" and "Cipher". It contains four rows, each with a radio button, a text input field for the encryption key, a dropdown menu for the cipher, and two radio buttons for "ASCII" and "HEX". The first row has the key "mysecretwepkey", the cipher set to "128 bits", and "ASCII" selected. The other three rows have empty key fields and "64 bits" selected for the cipher, with "ASCII" also selected. Below the key input fields, there is explanatory text: "Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits." and "Enter 5, 13, or 29 ASCII characters for 64, 128 or 256 bit Encryption Keys respectively. e.g.,ABCDE for a key length of 64 bits." A note at the bottom states: "Note: you must Restart Access Point for Wireless changes to take effect." At the bottom right, there are "Apply" and "Cancel" buttons.

Figure 7 (Wireless Security screen)

4.7 Save Settings

Press this button in order to permanently save the current configuration of the Wireless Gateway. If you do re-start the system without saving your configuration, the Wireless Gateway will revert back to the previously saved configuration.

Save Settings	
Save All	Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.

Figure 8 (Save Settings screen)

5. Advanced

This mode is catered for advance users, a brief explanation of the links are listed as shown in figure 9

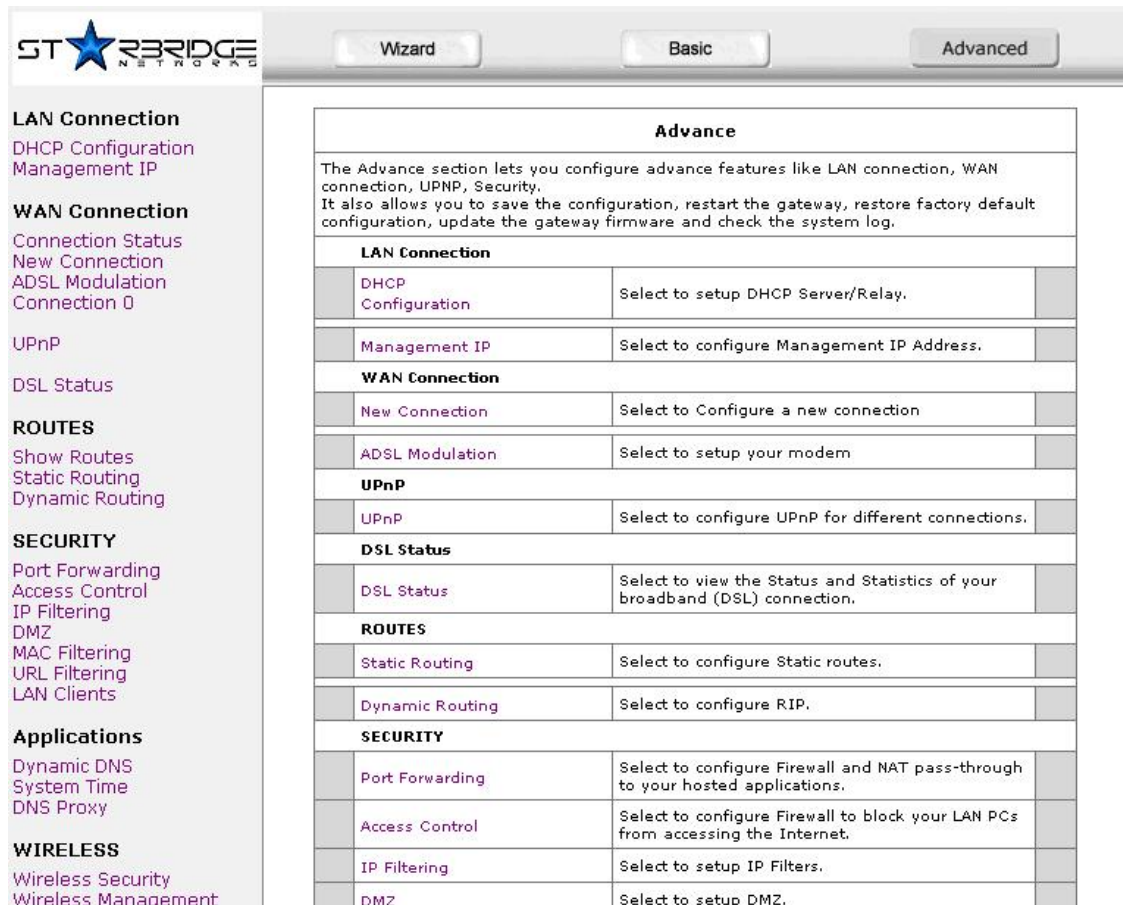


Figure 9 (Advanced screen)

5.1 LAN Connection

On one side of your Wireless Gateway, you have your own Local Area network (LAN) connections. This is where you plug in your local computers to the Wireless Gateway. The Wireless Gateway is normally configured to automatically provide all the PC's on your network with Internet addresses.

5.1.1 DHCP Configuration

To enable or disable DHCP, Click setup. Under LAN Setup, select DHCP Configuration. This will bring up the screen shown in Figure 10.

The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the Wireless Gateway IP address value. For example if the Wireless Gateway IP address is 192.168.1.1 (default) than the starting IP address must be 192.168.1. 2 (or higher).

The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254. Hence the max value for our default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users will not get access to network resources. If this happens you can increase the Ending IP address (to the limit of 255) or reduce the lease time.

The Lease Time is the amount of time a network user will be allowed connection to the Wireless Gateway with their current dynamic IP address. The amount of time is in units of minutes; the default value is 3600 minutes (60 hours).

Note: If you change the start or end values, make sure the values are still within the same subnet as the gateways IP address. In other words, if the gateways IP address is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.128.1.2/192.128.1.100, you will not be able to communicate to the Wireless Gateway if your PC has DHCP enabled.

DHCP Configuration

☒ Server On Start IP: 192.168.1.10
End IP: 192.168.1.200
Lease Time: 3600 Seconds

☐ Relay On Relay IP: 20.0.0.3

☐ Server and Relay Off

Apply Cancel

Figure 10 (DHCP Configuration screen)

In addition to the DHCP server feature, the Wireless Gateway supports the DHCP relay function. When the Wireless Gateway is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the Wireless Gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 11.

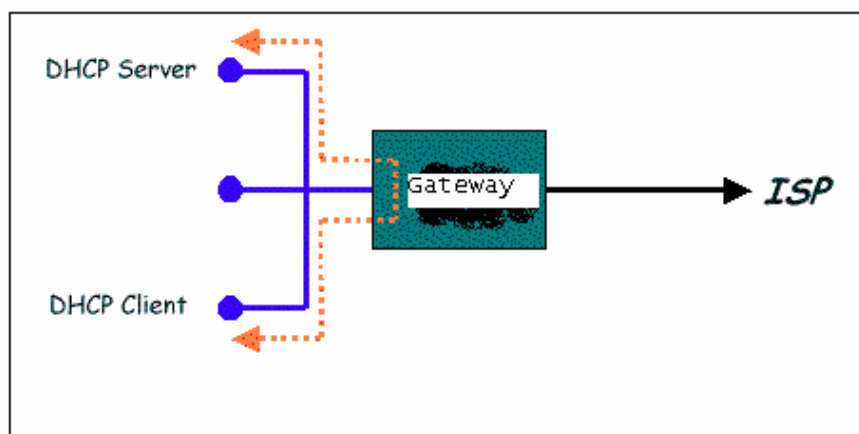


Figure 11 (Example of a DHCP Relay configuration)

By turning off the DHCP server and relay the network administrator must carefully configure the IP address, Subnet Mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer and your Wireless Gateway must be on the same subnet as all the other computers.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.1.2 Management IP (Changing the Wireless Gateway IP address)

You can change the Wireless Gateway's IP address by, clicking Setup and under LAN Setup, select Management. This will bring up the screen shown in Figure 12.

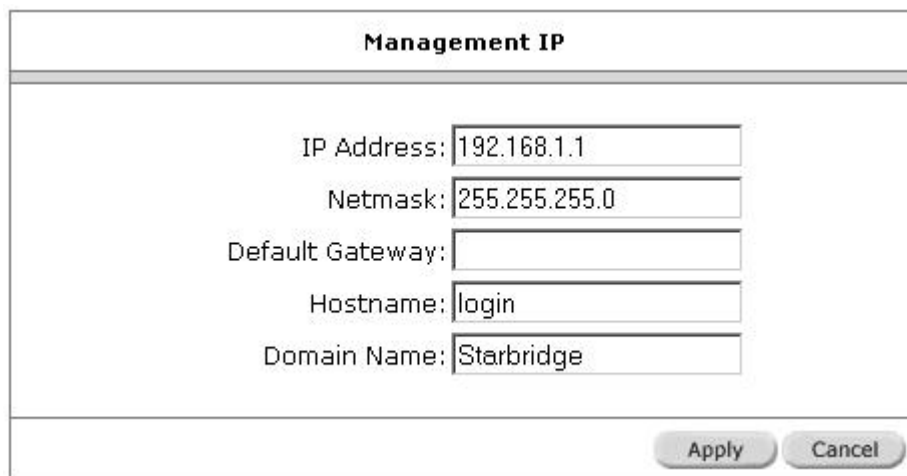
5.1.2.1 Static IP address assignment

Your Wireless Gateway's default IP address and subnet mask are 192.168.1.1/255.255.255.0; this subnet mask will allow the Wireless Gateway to support 254 users. If you want to support a larger number of users you can change the subnet mask; but remember. The DHCP server is defaulted to only give out 255 IP addresses. Further remember that if you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet

The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address. Figure 12 shows a default gateway address of 203.125.64.1 because this was the default gateway defined when the CLIP connection was configured.

The hostname can be any alphanumeric word that does not contain spaces. The domain name is used to in conjunction with the host name to uniquely identify the gateway. To access the Wireless Gateway's web pages the user can type 192.168.1.1 (the default IP address) or type mygateway.ar7.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.



The image shows a web-based configuration window titled "Management IP". It contains five input fields for network settings: "IP Address" with the value "192.168.1.1", "Netmask" with "255.255.255.0", "Default Gateway" which is empty, "Hostname" with "login", and "Domain Name" with "Starbridge". At the bottom right of the window are two buttons: "Apply" and "Cancel".

Figure 12 (Management IP)

5.2 WAN Connection

On the other side of the Wireless Gateway is where your Wide Area Network (WAN) connection; also referred to as a broadband connection. This WAN connection is different for every WAN supplier. Most of the configuration you will perform will be in this area. Local Area Network Connection(s)

5.2.1 Status

Status will display all the relevant information regarding your Internet Connection, it will display the type of protocol used, the WAN IP address, the connection state, the duration and if it is Disconnected the reason will be displayed. The “Disconnect” button on the right-hand side is for terminating the connection from the Internet.

Connection Status						
Description	Type	IP	State	Online	Disconnect Reason	
quickstart	pppoe	203.125.77.220	Connected	0hr 12min 36sec	N/A	Connect
						Refresh

Figure 13 (Connection Status Page)

5.2.2 Configuring the WAN

Before the gateway will pass any data between the LAN interface(s) and the WAN interface, the WAN side of the modem must be configured. Depending upon your DSL service provider or your ISP, you will need some (or all) of the information outlined below before you can properly configure the WAN:

- Your DSL line VPI and VCI
- Your DSL encapsulation type and multiplexing
- Your DSL training mode (default is MMODE)
- For PPPoA or PPPoE users, you also need these values from your ISP:
 - o Your username and password
- For RFC 1483 users, you may need these values from your ISP:
 - o Your DSL fixed Internet IP address
 - o Your Subnet Mask
 - o Your Default Gateway
 - o Your primary DNS IP address

Since multiple users can use the Wireless Gateway, the Wireless Gateway can simultaneously support multiple connection types; hence, the user must set up different profiles for each connection. The Wireless Gateway supports the following protocols:

- DHCP
- RFC2364 / PPPoA
- RFC2516 / PPPoE

- Static
- Bridged
- RFC1577 / CLIP

5.2.3 New Connection

A new connection is basically a virtual connection. Your Wireless Gateway can support up to 8 different (unique) virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the modem to pass data correctly

5.2.3.1 Bridged gateway profile and Connection

A pure bridged connection does not assign an IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the Wireless Gateway act as a hub, and just passes packets across the WAN interface to the LAN interface.

To configure the Wireless Gateway as a bridge, click on Setup and then click on **New Connection**. The default PPPoE connection setup is displayed. At the Type field select **Bridge** and the Bridge connection setup page is displayed (see Figure 4). Give your Bridge connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called **Bridge**. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using **0,100**. Also select the quality of service (QoS); leave the default value if you are unsure or the ISP did not provide this information.

Bridged Connection Setup

Name: Type:

Bridge Settings

Encapsulation: ☒ LLC ☐ VC

PVC Settings

VPI:
VCI:
QoS:
PCR: cps
SCR: cps

Figure 14 (Bridge Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent, you need to click on **Save Settings**. At the system commands page, click on **Save All**.

5.2.3.2 PPPoA Connection Setup

PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets over ATM cells which are carried over the DSL line. PPP or Point-to-Point protocol is a method of establishing a network connection / session between network hosts. It usually provides a mechanism of authenticating users. LLC and VC are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

By selecting PPPoA, you are forcing your Wireless Gateway to terminate the PPPoA connection. The advantage is that the PPPoA termination is done within the Wireless Gateway and not on your PC; this frees up your PC resources and allows multiple users to utilize the PPPoA connection.

To configure the gateway for PPPoA, click on Setup and then click on **New Connection**. The default PPPoE connection setup is displayed. At the Type field select **PPPoA** and the PPPoA connection setup page is displayed; figure 5 illustrates a typical PPPoA configuration. Give your PPPoA connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called **PPPoA1**. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using **0,100**. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

Following is a description of the different options:

- a. Username: The username for the PPPoA access; this is provided by your DSL service provider or your ISP.
- b. Password: The password for the PPPoA access; this is provided by your DSL service provider or your ISP.
- c. On-Demand: Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
- d. Idle Timeout: Specifies that PPPoA connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a 0 in this field.
- e. Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
- f. Set Route: Specify this connection as the default-route.

MRU: Maximum Receive Unit the DSL connection can receive. It is a negotiated value that asks the provider to send packets of no more than n bytes. The maximum specified value is 1500 although some DSL/ISP providers require a larger value. The minimum MRU value is 128.

PPPoA Connection Setup

Name: Type:

Options: ☒ NAT ☒ Firewall

PPP Settings

Encapsulation: ☒ LLC ☐ VC

Username:

Password:

Idle Timeout: secs

Keep Alive: min

Authentication: ☒ Auto ☐ CHAP ☐ PAP

MAX Fail: times

MRU: bytes

On Demand: ☐ Set Route: ☒

PVC Settings

VPI:

VCI:

QoS:

PCR: cps

SCR: cps

Figure 15 (PPPoA Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Setting** (at the side of the page). At the system commands page, click on **Save All**.

5.2.3.3 PPPoE Connection Setup

PPPoE is also known as RFC 2516. It is a method of encapsulating PPP packets over Ethernet. PPP or Point-to-Point protocol is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users.

To configure the gateway for PPPoE, click on Setup and then click on **New Connection**. The default PPPoE connection setup is displayed. At the Type field select **PPPoE** and the PPPoE connection setup page is displayed; figure 6 illustrates a typical PPPoE configuration. Give your PPPoE connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called **PPPoE1**. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using **0,100**. Also select the quality of service (QoS); leave the default value if you are unsure or the ISP did not provide this information.

Following is a description of the different options:

- a. Username: The username for the PPPoE access; this is provided by your DSL service provider or your ISP.

- b. Password: The password for the PPPoE access; this is provided by your DSL service provider or your ISP.
- c. On-Demand: Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
- d. Idle Timeout: Specifies that PPPoE connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a 0 in this field.
- e. Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
- f. Set Route: Specify this connection as the default-route.
- g. MRU: Maximum Receive Unit the DSL connection can receive. It is a negotiated value that asks the provider to send packets of no more than n bytes. The maximum specified value is 1500 although some DSL/ISP providers require a larger value. The minimum MRU value is 128.
- h. Enforce MRU: Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MRU by changing TCP Maximum Segment Size to PPP MRU.

PPPoE Connection Setup

Name: Type:

Options: ☒ NAT ☒ Firewall

PPP Settings

Username:

Password:

Idle Timeout: secs

Keep Alive: min

Authentication: ☒ Auto ☐ CHAP ☐ PAP

MAX Fail: times

MRU: bytes

On Demand: ☐ Set Route: ☒

Enforce MRU: ☒

PVC Settings

VPI:

VCI:

QoS:

PCR: cps

SCR: cps

Figure 16 (PPPoE Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Setting** (at the side of the page). At the system commands page, click on **Save All**.

5.2.3.4 DHCP Connection Setup

Dynamic Host Configuration Protocol (DHCP) allows the Wireless Gateway to automatically obtain the IP address from the server. This option is commonly used in situations where IP is dynamically assigned and is not known prior to assignment.

To configure the Wireless Gateway for a DHCP connection, click on Setup and then click on **New Connection**. The default DHCP connection setup is displayed. At the Type field select **DHCP** and the DHCP connection setup page is displayed; figure 7 illustrates a typical DHCP configuration. Give your DHCP connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called **DHCP1**. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using **0,100**. Also select the quality of service (QoS); leave the default value if you are unsure or the ISP did not provide this information.

If your DSL line is connected and your DSL/IPS provider is supporting DHCP, you can click the renew button and the gateway will retrieve an IP address, Subnet mask, and Gateway address. At anytime, you can renew the DHCP address by clicking on the renew button; in most cases you will never have to use this button.

Figure 17 (DHCP Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.3.5 Static Connection Setup

Static is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers would enable you to have access to other web servers. Valid IP addresses range is from 0.0.0.0 to 255.255.255.255.

To configure the Wireless Gateway for a Static connection, click on Setup and then click on **New Connection**. The default Static connection setup is displayed. At the Type field select **Static** and the Static connection setup page is displayed; figure 8 illustrates a typical Static configuration. Give your Static connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called **STATIC1**. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using **0,100**. Also select the quality of service (QoS); leave the default value if you are unsure or the ISP did not provide this information. You can also enable Network Address Translation (NAT) and the Firewall options. If you are unsure, leave these in the default mode.

Based upon the information your DSL/ISP provided, enter your assigned IP address, Subnet Mask, Default Gateway (if provided), and Domain Name Services (DNS) values (if provided). For the static configuration, you can also select a bridge connection or a routed connection. Since static IP address is typically used to host WEB servers, you may want to use a bridge connection.

Figure 18 (Static IP Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.3.6 Classical IP over ATM (CLIP, defined in RFC1577) Connection Setup

The Classical IP over ATM (CLIP) support provides the ability to transmit IP packets over an ATM network, CLIP support will encapsulate IP in an AAL5 packet data unit (PDU) frame using RFC1577 and it utilizes an ATM aware version of the ARP protocol (ATMARP). support only allows for PVC support; it does not support SVC).

To configure the Wireless Gateway for a CLIP connection, click on Setup and then click on **New Connection**. The default CLIP connection setup is displayed. At the Type field select **CLIP** and the CLIP connection setup page is displayed; figure 9 illustrates a typical CLIP configuration. Give your CLIP connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called **CLIP1**. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using **0,101**. Also select the quality of service (QoS); leave the default value if you are unsure or the ISP did not provide this information. You can also enable Network Address Translation (NAT) and the Firewall options. If you are unsure, leave these in the default mode.

CLIP Connection Setup

Name: Type:

Options: ☒ NAT ☒ Firewall

CLIP Settings

IP Address:
Mask:
ARP Server:
Default Gateway:

PVC Settings

VPI:
VCI:
QoS:
PCR: cps
SCR: cps

Apply Delete Cancel

Figure 19 (CLIP Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.4 Modify an Existing Connection

To modify an existing connection, click setup and then click the connection you want to modify. The connections are listed as Connection 0 through Connection 7

As a note, if you delete the connection, to make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.5 Modem setup

To configure the DSL modulation type, Click setup. Under WAN Setup, select Modem Setup. This will bring up the modem setup screen. Leave the default value if you are unsure or the DSL/ISP did not provide this information. For most all cases, this screen should not be modified.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.6 Firewall/NAT Services

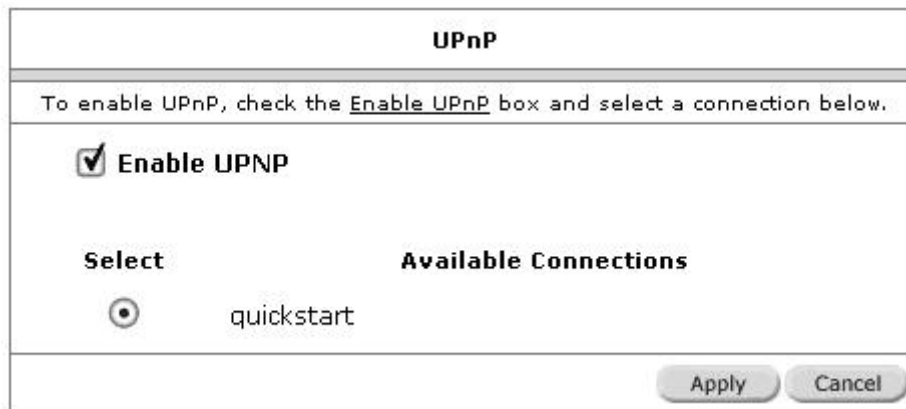
You can enable or disable Firewall and NAT by clicking on Setup and under LAN Setup, select Firewall/NAT Services. By unselecting the “Enable Firewall and NAT Services” button the firewall and NAT services is disabled for all WAN connections.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.7 UPnP

UPnP NAT and Firewall Traversal allow traffic to pass-thru the Wireless Gateway for applications using the UPnP protocol. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over, which the incoming traffic will be present, for example the default Internet connection.

To enable UPnP, you must first have a WAN connection configured. Once a WAN connection is configured, click Advanced and under Advanced, select UPnP. This will bring up the screen shown in Figure 13. You must enable UPnP and then select which connection will utilize UPnP. In this case the PPPoA connection is enabled.



UPnP	
To enable UPnP, check the <u>Enable UPnP</u> box and select a connection below.	
☒ Enable UPnP	
Select	Available Connections
☐	quickstart
Apply Cancel	

Figure 20 (UPNP screen)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.2.8 Modem Status

This screen will display the Modem status and DSL statistics

Modem Status	
Modem Status	
Connection Status	Connected
Us Rate (Kbps)	448
Ds Rate (Kbps)	3488
US Margin	15
DS Margin	12
Modulation	MMODE
LOS Errors	0
DS Line Attenuation	34
US Line Attenuation	37
Path Mode	Fast Path
DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0
Refresh	

Figure 21 (Modem Status screen)

5.3 Routes

5.3.1 Show Routes

Routing Table shows the information used by routers when making packet forwarding decisions. Packets are routed according to the packet's destination IP address

Routing Table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0

Figure 22 (Modem Status screen)

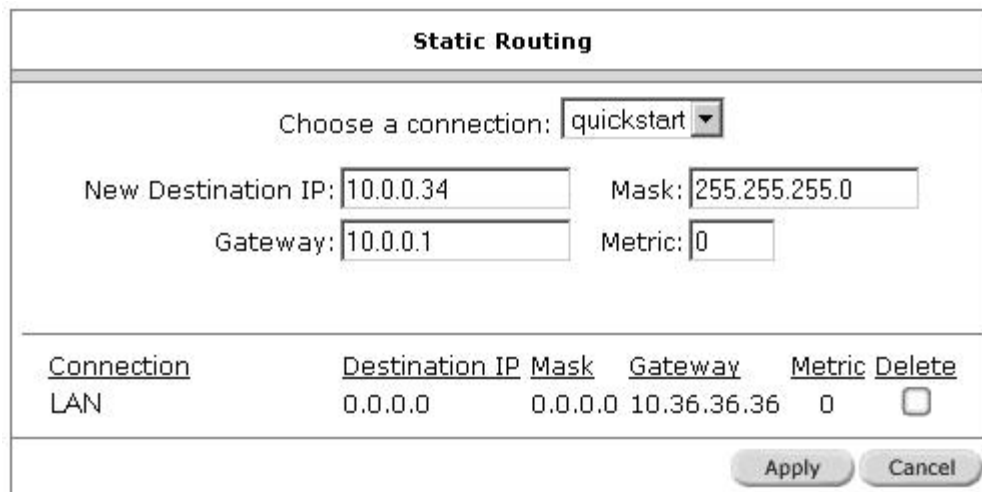
5.3.2 Static Routing

If the Wireless Gateway is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the Wireless Gateway.

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route

here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host. The Hop Count determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network (such as a router or switch)

To enable Static Routing, from the Home screen, click Advanced and under Advanced, select Static Routing. Figure 22 illustrates a typical Static Route



The image shows a 'Static Routing' configuration window. At the top, it says 'Choose a connection:' with a dropdown menu showing 'quickstart'. Below this, there are four input fields: 'New Destination IP:' with the value '10.0.0.34', 'Mask:' with the value '255.255.255.0', 'Gateway:' with the value '10.0.0.1', and 'Metric:' with the value '0'. At the bottom, there is a table with columns: 'Connection', 'Destination IP', 'Mask', 'Gateway', 'Metric', and 'Delete'. The table has one row with the values: 'LAN', '0.0.0.0', '0.0.0.0', '10.36.36.36', '0', and a checkbox. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Connection	Destination IP	Mask	Gateway	Metric	Delete
LAN	0.0.0.0	0.0.0.0	10.36.36.36	0	☐

Figure 23 (Static Routing)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.3.3 Dynamic Routing

Dynamic Routing allows the Wireless Gateway to automatically adjust to physical changes in the network. The Wireless Gateway, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Wireless Gateways on the network.

The Direction determines the direction that RIP routes will be updated. Selecting In means that the Wireless Gateway will only incorporate received RIP information. Selecting Out means that the Wireless Gateway will only send out RIP information. Selecting both means that the Wireless Gateway will incorporate received RIP information and send out updated RIP information.

The protocol is dependent upon the entire network. Most networks support Rip v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If Rip V2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If Rip V1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting.

To enable Dynamic Routing, click Advanced and under Advanced, select Dynamic Routing. Figure 18 illustrates a typical Dynamic Route.

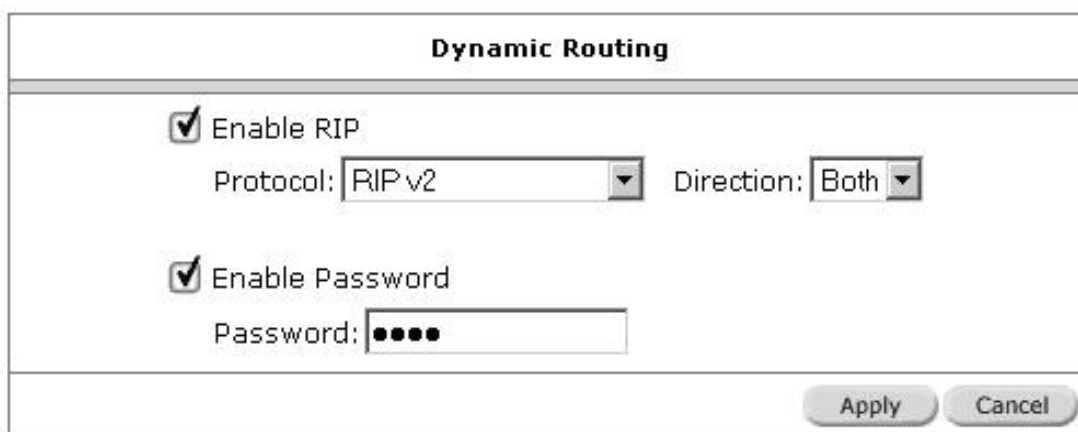
A screenshot of a 'Dynamic Routing' configuration window. The window has a title bar 'Dynamic Routing'. Inside, there are two checked checkboxes: 'Enable RIP' and 'Enable Password'. Below 'Enable RIP', there is a 'Protocol:' label followed by a dropdown menu showing 'RIPv2' and a 'Direction:' label followed by a dropdown menu showing 'Both'. Below 'Enable Password', there is a 'Password:' label followed by a text box containing four dots. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Figure 24 (Dynamic Routing)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.4 Security

5.4.1 Port Forwarding

Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. When users send this type of request to your network via the Internet, the Wireless Gateway will forward those requests to the appropriate PC. Port forwarding can be used with DHCP assigned addresses but remember that a DHCP address is dynamic (not static). For example, if you were configuring a Netmeeting server, you would want to assign this server a static IP address so that the IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. The port forwarding will translate the WAN IP address into a LAN IP address.

To configure a service, game, or other application select the external connection (for example the Internet connection), from the Home screen, click Advanced and under Advanced, select Port Forwarding. Next select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click New and fill in the port, protocols and description for your application.

For example, if you want to host a Netmeeting session, from the Home screen, click Advanced and under Advanced, select Port Forwarding. First select the IP address for your Netmeeting server. Next select the Audio/Video category and add Netmeeting to the applied rules box. To view the management rules, highlight Netmeeting and select view; this will display the pre configured protocols and ports that Netmeeting will use. Now assuming that your WAN connection is correct, you can run Netmeeting from your server and call users that are on the Internet. If you know your WAN IP address, users can call you.

Port Forwarding

Choose a connection: quickstart

LAN IP: 192.168.1.10 New IP Custom Rules

Category	Available Rules		Applied Rules
☐ Games	Net2Phone	Add > < Remove	Asheron's Call
☐ VPN	Netmeeting		Netmeeting
☒ Audio/Video	Quick Time 4 Server		
☐ Apps			
☐ Servers			
☐ User			

Apply Cancel

Figure 25 (Port Forwarding)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.4.2 Access Control

Access control can also be called port blocking. It has the functionality opposite to Port Forwarding. Specific types of traffic that is destined to a selected LAN IP address can be blocked. To enable any of the Access Control features, click Advanced and under Advanced, select Access Control. A page similar to the port-forwarding page appears. Similar to the port-forwarding page, an IP address can be added to a rule. All Access Control rules have precedence over rules that were added via the port-forwarding page.

The example shown in (figure 25) demonstrates that all the ports for this particulate LAN IP is block, the workstation will not be able to access the WAN traffic.

Access Control

LAN IP: 192.168.1.10 New IP

Block All Traffic: ☒ Custom Rules

Category	Available Rules	Applied Rules
☐ Games ☐ VPN ☒ Audio/Video ☐ Apps ☐ Servers ☐ User	Net2Phone Netmeeting Quick Time 4 Server View	Netmeeting Add > < Remove

Apply Cancel

Figure 26 (Access Control screen)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

5.4.3 IP Filter

IP filter is identical to what Port blocking to Access Control. In (figure 26) it demonstrates that the router will block workstations with the IP in the defined range of 192.168.1.5 to 192.168.1.20 and port range from 2000 to 3000.

IP Filter

Filter Name: blockrange Enable: ☒

Source IP Start: 192.168.1.10 Source IP End: 192.168.1.20

Port Start: 2000 Port End: 3000

Protocol: TCP and UDP

Enabled	Name	Source IP Start	Source IP End	Source Port Start	Source Port End	Protocol	Edit	Delete

Apply Cancel

Figure 27 (IP Filter screen)

5.4.4 DMZ

5.4.4.1 DMZ configuration

Setting a computer (on your local network) as a DMZ forwards any network traffic that is not redirected to another computer via the port-forwarding feature to the computer's IP address. This opens the access to the DMZ computer from the Internet.

5.4.4.2 Enable Web from WAN

Enabling the Web from WAN on your local network allows Web requests that come from the Internet to be re-routed to a Web Server that is on a different subnet. This is different that the Web server rule that is configurable via the port-forwarding page. In this case, the web server is on a different subnet.

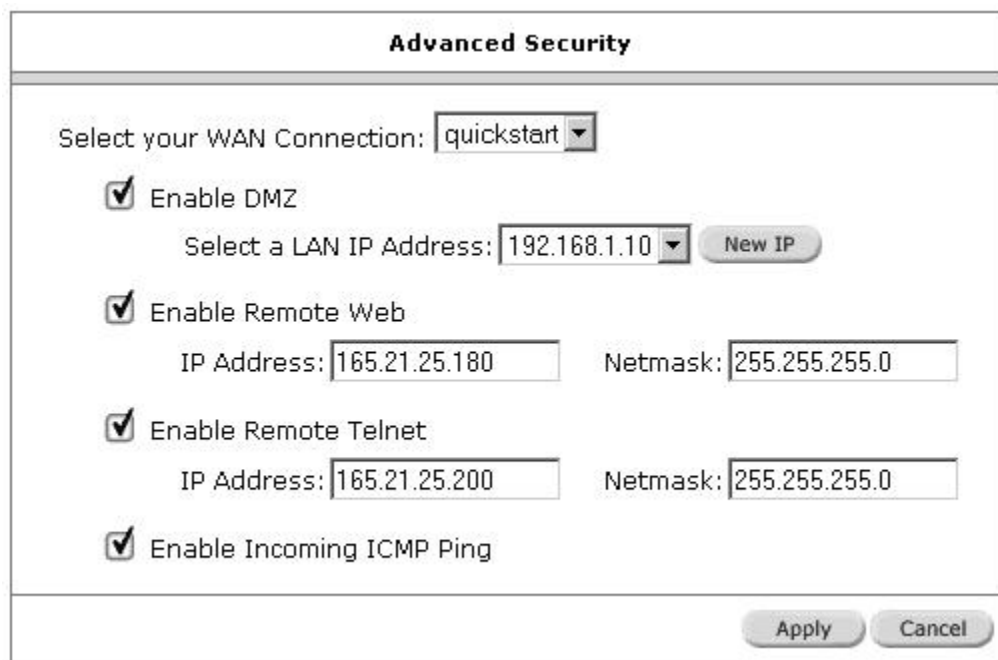
5.4.4.3 Enable Remote Telnet

Enabling the Remote Web on your local network allows telnet requests that come from the Internet to be re-routed to a telnet Server that is on a different LAN IP subnet. This is different that the telnet server rule that is configurable via the port-forwarding page. In this case, the telnet server is on a different subnet.

5.4.4.4 Enable Incoming ICMP Ping

Enabling the Incoming Internet Control Message Protocol (ICMP) Ping will allow Echo requests to come into the gateway. The gateway will respond with an ICMP Echo response message. The option allows the DSL provider or ISP to determine the following:

- a. The status of the network.
- b. Tracking and isolating hardware and software problems.
- c. Testing, measuring, and managing networks.



The image shows a screenshot of the 'Advanced Security' configuration window. At the top, the title 'Advanced Security' is centered. Below the title, there is a dropdown menu labeled 'Select your WAN Connection:' with 'quickstart' selected. Below this, there are four checked checkboxes, each followed by a label and input fields. The first checkbox is 'Enable DMZ', followed by 'Select a LAN IP Address:' with a dropdown showing '192.168.1.10' and a 'New IP' button. The second checkbox is 'Enable Remote Web', followed by 'IP Address:' with a text box containing '165.21.25.180' and 'Netmask:' with a text box containing '255.255.255.0'. The third checkbox is 'Enable Remote Telnet', followed by 'IP Address:' with a text box containing '165.21.25.200' and 'Netmask:' with a text box containing '255.255.255.0'. The fourth checkbox is 'Enable Incoming ICMP Ping'. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Figure 28 (Advanced Security screen)

5.4.5 MAC Filter

The MAC filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the defined filter rules sequentially, and when a matched is determined, the appropriate filtering action (determined by the access type selected ... i.e. allow or deny) is performed. The user should note that the MAC filter will only examined frames from interfaces that are part of the bridge itself. Twenty filter rules are supported with MAC filtering. To enable MAC Filters, click Advanced and under Advanced, select MAC Filters. Figure 15 illustrates a typical Bridge filter configuration.

The User Interface for MAC Filter allows the user to add/edit/delete, as well as, enables the filter rules. To add rules, simply define the source MAC address, destination MAC address and frame type with desired filtering type (i.e. allow/deny), and press the "Add" button. The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as "don't care". Blanks can be used in the MAC address space, and would be considered also as "don't care".

To edit/modify an existing filter rule, select the desired rule created previously from "Add" in the "Edit" select box. The selected filter rule will appear on top section, as with the "Add" filter rule. Make the desired change to the MAC address, frame type and/or access type, and press "Apply".

To delete filter rule(s), select the filter rule entry to delete in the "Delete" selection box. Note that multiple deletions are possible. Once all the desired filter rule(s) is/are selected for deletion, press the "Apply" button. The "Select All" select box can also be used to delete the entire filter rule. It provides a quick method of selecting all filter rules for deletion.

The "Enable MAC Filters" button allow the user to enable or disable MAC filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the "Apply" button.

Note: The MAC filter table contains 3 hidden rules. These rules are entered automatically by the system to ensure the user does not "lock" them out of the system. The first rule allows any and all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the bridge to go through. The third rule allows all IPv4 frames with the source MAC address of the bridge to go through.

Note: On a windows based machine, to find a MAC address, at a dos prompt type **ipconfig /all**.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

MAC Filters

☐ **Enable MAC Filters**

Source MAC	Destination MAC	Protocol	Mode
00-00-00-00-00-00 e.g AB-AB-AB-AB-AB-AB	00-00-00-00-00-00 e.g AB-AB-AB-AB-AB-AB	Any	Deny

Edit	Source MAC	Destination MAC	Protocol	Mode	Delete
☐	00-00-00-00-00-00	00-00-00-00-00-00	Any	Deny	☐
				Select All	☐

Figure 29 (MAC Filter screen)

5.4.6 LAN clients

To add a LAN client, click Advanced and under Advanced, select LAN Clients. If DHCP is used, all DHCP clients are automatically assigned. If a fixed IP address server is on the LAN and you want this server to be visible via the WAN, you must add its IP address. Once the IP address has been added to you can apply Port Forwarding and Access Control rules to this IP address.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

LAN Clients

New IP Address:

Hostname:

Static Addresses

<u>Delete</u>	<u>IP Address</u>	<u>Hostname</u>	<u>Type</u>
Dynamic Addresses			
<u>Reserve</u>	<u>IP Address</u>	<u>Hostname</u>	<u>Type</u>
☐	192.168.1.10	oem-i0s17j2t0xq	Dynamic

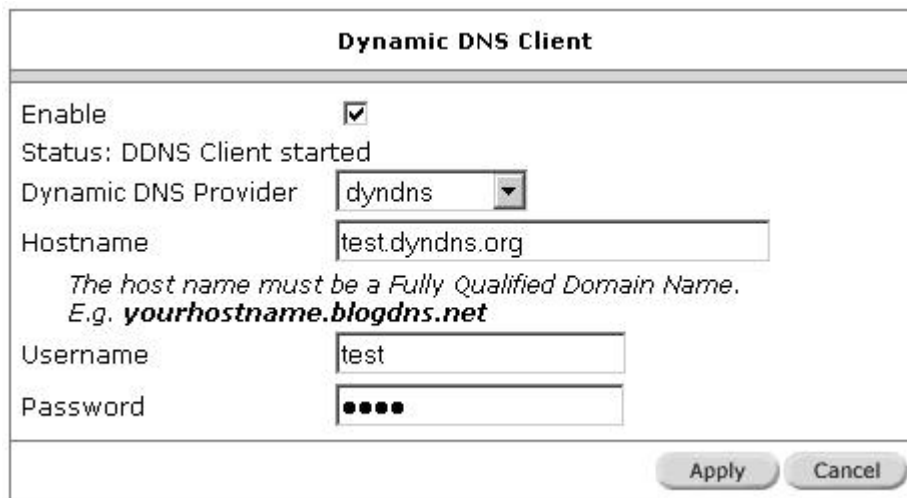
Figure 30 (LAN Clients)

5.5 Applications

5.5.1 Dynamic DNS

Dynamic DNS allows the user to register with a Dynamic DNS Provider as listed. The dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services.

*note: The Username/Password entered should be similar to the Username/Password you have specified during the registration of the DNS hostname.



The screenshot shows a window titled "Dynamic DNS Client". It contains the following fields and controls:

- Enable:** A checkbox that is checked.
- Status:** A text label indicating "DDNS Client started".
- Dynamic DNS Provider:** A dropdown menu with "dyndns" selected.
- Hostname:** A text input field containing "test.dyndns.org". Below this field is a note: "The host name must be a Fully Qualified Domain Name. E.g. **yourhostname.blogdns.net**".
- Username:** A text input field containing "test".
- Password:** A text input field with four dots representing a masked password.
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

Figure 31 (Dynamic DNS)

5.5.2 System Time

This feature allows the time in the router to be synchronizing with a specified Time server.

The "system log" and "current time" will be able to reflect the updated time upon successfully connected the time server

System Time Configuration	
The Router keeps time by connecting to a Network Time Protocol (NTP) server. This allows the Router to synchronize the system clock to the Internet. The system clock can only be updated if there is a connection to the Internet and the configured time server is up and available. Please allow about 15 minutes for the Router to contact a time server and get a response.	
Current Time: 0:55:34	
Enable	☒
Time Zone	(GMT+08:00) Perth
Time Server	ntp.shim.org (optional)
You can enter the DNS or IP address of an optional timeserver of your choice here. Leave this blank to use the system's default server time.nist.gov.	
Apply Cancel	

Figure 32 (System Time)

5.5.3 DNS Proxy Settings

This feature allows the user to select the (Domain Name Server) DNS Server Priority as well as enter IP addresses for Primary DNS and secondary DNS

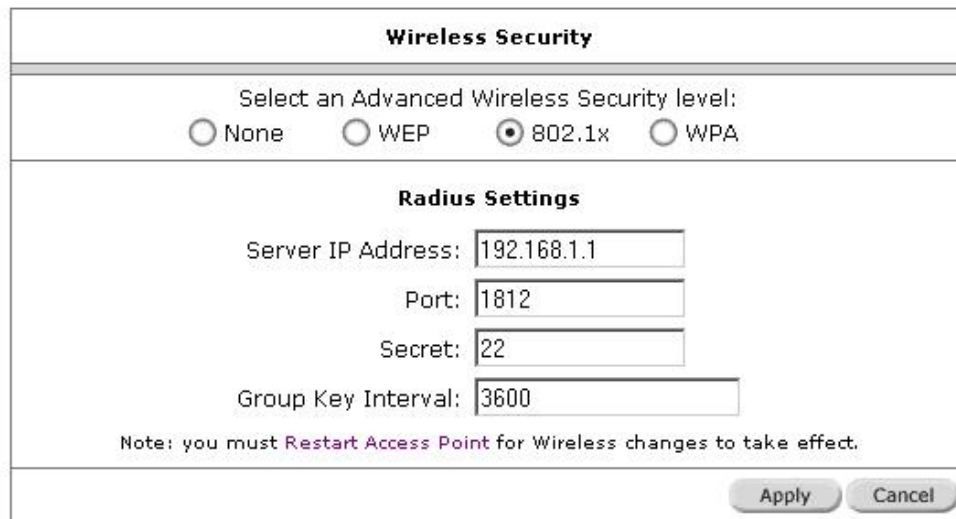
DNS Proxy Settings	
DNS Server Priority:	Only Auto Discovered DNS Servers
User Configured DNS Servers	
Primary DNS:	
Secondary DNS:	
Apply Cancel	

Figure 33 (DNS Proxy Settings)

5.6 Wireless

5.6.1 Wireless Security (Advance)

Enter the IP Address of the RADIUS Server (for 802.1x authentication purposes). This is used only when you have a RADIUS Server and want to use it for authentication. Almost all homes and offices do not have a RADIUS Server.



The screenshot shows the 'Wireless Security' configuration window. At the top, it says 'Wireless Security'. Below that, it asks to 'Select an Advanced Wireless Security level:' with four radio buttons: 'None', 'WEP', '802.1x' (which is selected), and 'WPA'. Underneath, there is a section titled 'Radius Settings' with four input fields: 'Server IP Address' (192.168.1.1), 'Port' (1812), 'Secret' (22), and 'Group Key Interval' (3600). A note at the bottom states: 'Note: you must Restart Access Point for Wireless changes to take effect.' At the very bottom are 'Apply' and 'Cancel' buttons.

Figure 34.1 (Wireless Security 802.1x screen)

WPA which stands for WiFi Protected Access. WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys.



The screenshot shows the 'Wireless Security' configuration window with 'WPA' selected. It says 'Wireless Security' at the top. Below, it asks to 'Select an Advanced Wireless Security level:' with four radio buttons: 'None', 'WEP', '802.1x', and 'WPA' (which is selected). Underneath, there is a 'Group Key Interval' input field with the value 3600. A note below it says: 'Note: Group Key Interval is shared by all WPA options.' Below that, there are two sections. The first is for '802.1x' (radio button is unselected) with fields for 'Server IP Address', 'Port' (1812), and 'Secret'. The second is for 'PSK String' (radio button is unselected) with a 'String' field. A note at the bottom states: 'Note: you must Restart Access Point for Wireless changes to take effect.' At the very bottom are 'Apply' and 'Cancel' buttons.

Figure 34.2 (Wireless Security WPA screen)

5.6.2 Wireless Management

The Wireless Management consist of Access List, Associated Stations and Multiple SSID features.

5.6.2.1 Access List

This feature permits you to “Allow” or “Ban” any wireless client from accessing the wireless router. You must add the MAC address of the client’s wireless LAN card.

Note: You must restart the Wireless Access Point to activate the changes for the wireless settings to take effect.



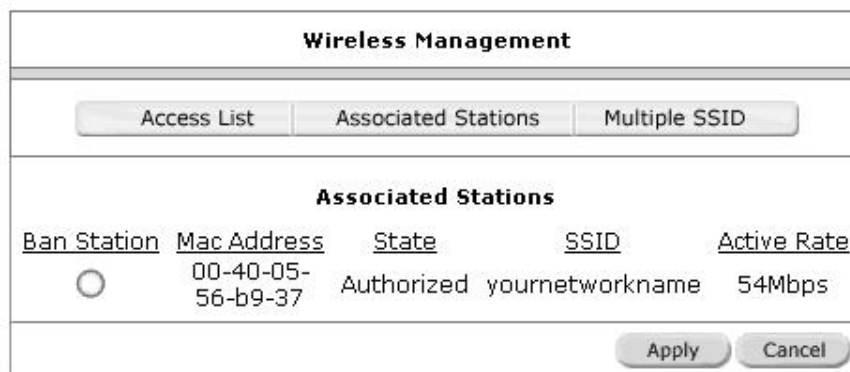
The screenshot shows the 'Wireless Management' interface with three tabs: 'Access List', 'Associated Stations', and 'Multiple SSID'. The 'Access List' tab is selected. It contains a section titled 'Access List' with an 'Enable Access List' checkbox (unchecked). Below it are two radio buttons: 'Allow' (selected) and 'Ban'. A 'Mac Address' input field is followed by an 'Add' button. Below the input field is a 'Delete' button and a 'Mac Address' label. A note states: 'Note: you must Restart Access Point for Wireless changes to take effect.' At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 35.1 (Wireless Management Access List screen)

5.6.2.2 Associated Stations

Wireless client which are connected to the wireless router will be displayed in this screen. You are able to ban this station by clicking on the “Ban Station” option. Then click on “Apply” button.

Note: You must restart the Wireless Access Point to activate the changes for the wireless settings to take effect.



The screenshot shows the 'Wireless Management' interface with three tabs: 'Access List', 'Associated Stations', and 'Multiple SSID'. The 'Associated Stations' tab is selected. It contains a section titled 'Associated Stations' with a table. The table has five columns: 'Ban Station', 'Mac Address', 'State', 'SSID', and 'Active Rate'. There is one row of data. Below the table are 'Apply' and 'Cancel' buttons.

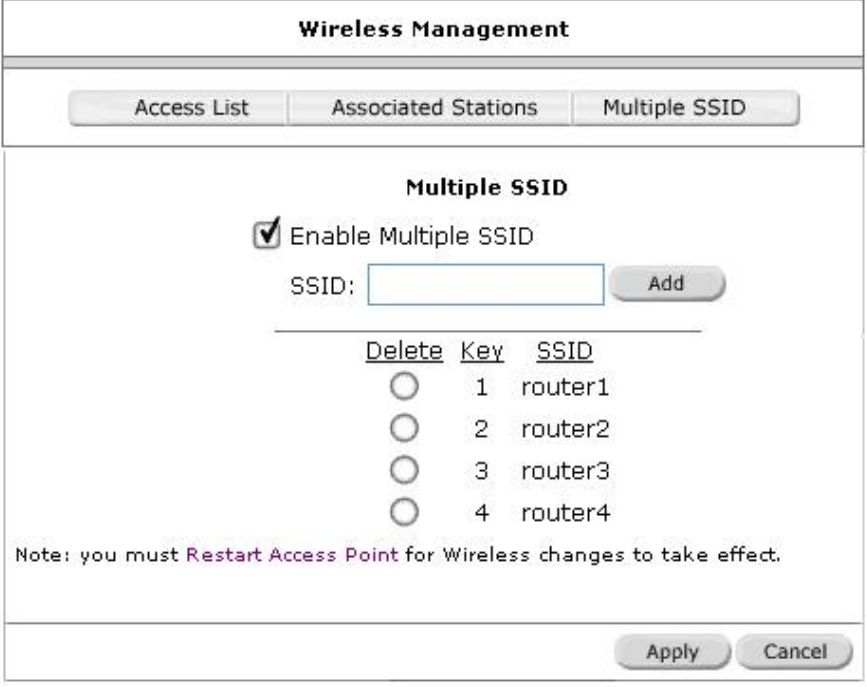
Ban Station	Mac Address	State	SSID	Active Rate
☐	00-40-05-56-b9-37	Authorized	yournetworkname	54Mbps

Figure 35.2 (Wireless Management Associated Stations screen)

5.6.2.3 Multiple SSID

This router supports multiple SSID, which means that you can set more than one SSID for this router.

Note: You must restart the Wireless Access Point to activate the changes for the wireless settings to take effect.



The screenshot shows the 'Wireless Management' interface with three tabs: 'Access List', 'Associated Stations', and 'Multiple SSID'. The 'Multiple SSID' tab is active. It features a checkbox labeled 'Enable Multiple SSID' which is checked. Below this is an 'SSID:' input field followed by an 'Add' button. A table lists four existing SSIDs, each with a radio button for selection. The table has columns for 'Delete', 'Key', and 'SSID'. At the bottom, there is a note about restarting the access point and 'Apply' and 'Cancel' buttons.

Delete	Key	SSID
☐	1	router1
☐	2	router2
☐	3	router3
☐	4	router4

Note: you must Restart Access Point for Wireless changes to take effect.

Figure 35.3 (Wireless Management Multiple SSID screen)

5.6.3 User Management

5.6.3.1 HTTP Authentication

There are two types of user for this wireless router "Admin" and "Normal". "Admin" user will be have administrator rights which can have access to "Wizard", "Basic" and "Advanced" tabs. However for "Normal" user, they can have access to "Wizard", "Basic" tabs.

You can change your Wireless Gateway's username and password by clicking on User Management. From here you can change the login name and password for Admin and Normal User. You can also change the idle timeout; you will need to log back onto the Wireless Gateway once the timeout expires.

If you forget your password, you can press and hold the reset to factory defaults button for 10 seconds (or more). The Wireless Gateway will reset to its factory default configuration and all custom configurations will be lost.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Save Settings** (at the side of the page). At the system commands page, click on **Save All**.

User Management	
User Management is used to change your User Name or Password.	
Enable Authentication: ☒	
Admin User Name:	admin (Max. 15 chars)
Admin Password:	(Max. 15 chars)
Confirmed Admin Password:	(Max. 15 chars)
Normal User Name:	user (Max. 15 chars)
Normal Password:	(Max. 15 chars)
Confirmed Normal Password:	(Max. 15 chars)
Idle Timeout:	30 minutes
Apply Cancel	

Figure 36 (HTTP Authentication screen)

5.6.3.2 Firmware Update

You can upgrade the Wireless Gateway's firmware, clicking on Update Firmware under the **Tools** page. This will bring up the screen shown in Figure 33.1. The upgrade file shall be in *.img format.

To upgrade the firmware, click browse, find the firmware file to download. Make sure this is the correct file. Click on upgrade firmware (as shown in Figure 19). Once the upgrade is complete the Wireless Gateway will reboot. You will need to log back onto the Wireless Gateway after the firmware upgrade is completed.

The firmware upgrade should take about 5 minutes to complete.

Note: Do not remove power from the Wireless Gateway during the firmware upgrade procedure.

Update Firmware	
To update your gateway firmware, choose an update image (Kernel/Filesystem) or configuration file in Select a File, and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.	
Select a File:	Examinar...
Update Gateway	
The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.	
Get Configuration	
Status:	None

Figure 37.1 (Firmware Update screen)

5.6.3.3 Restore Default Settings

Restore Defaults: Use this button to restore factory default configuration.

NOTE: Connectivity to the router will be lost. You will be re-connected to the router after the unit reboots.



Figure 37.2 (Restore Default Settings screen)

5.6.3.4 Restart Router

Use this button to re-start the system. If you have not saved your configurations, the Wireless Gateway will revert back to the previously saved configuration upon re-starting.

NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots

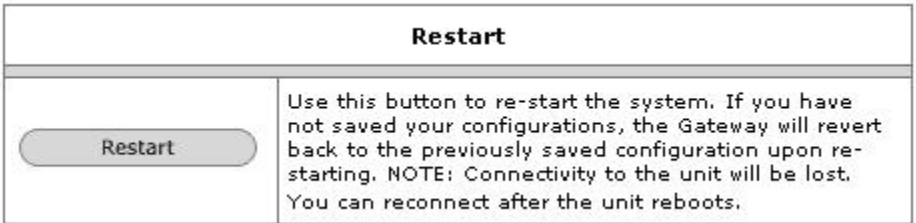


Figure 37.3 (Restart Router screen)

5.6.3.5 System Log

You can display the Wireless Gateway's log by going under the Status title, click System log. From here you can view all logged information. Depending upon the severity level, this logged info will generate log reports to a remote host (if remote logging is enabled).

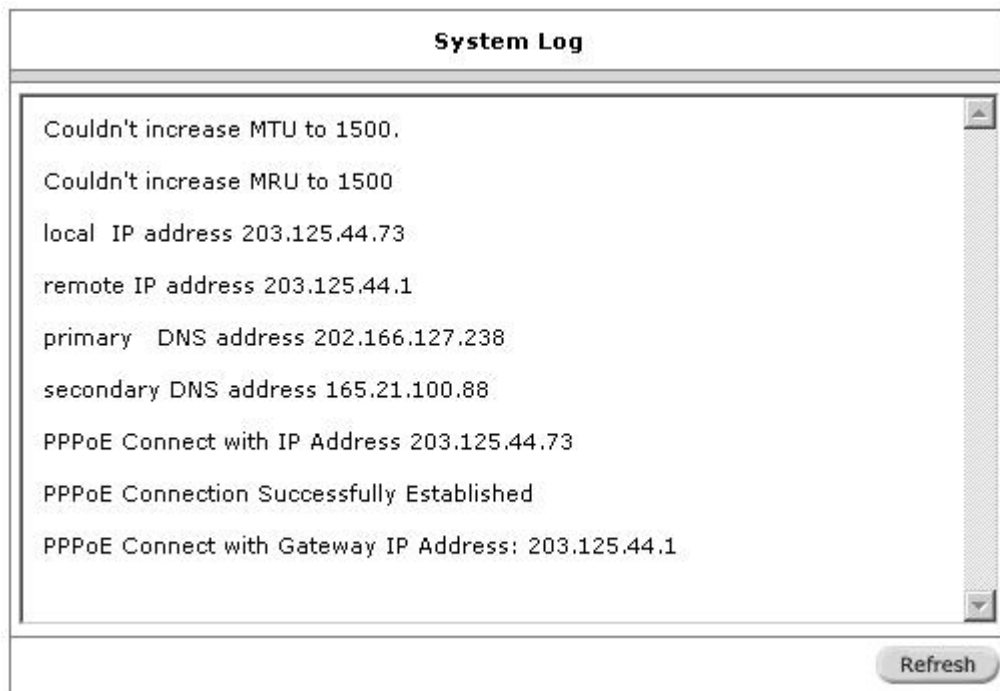


Figure 37.4 (System Log screen)

6. Appendix A: Troubleshooting

Below is a list of commonly asked questions. Before calling technical support, please look through these issues to see if they help to solve your problem.

6.1 The Wireless Gateway is not functional

1. Check to see that the power LED is green and than the network cables are installed correctly. Refer to the easy start guide for more details.
2. Check to see that the ETH and Internet LEDs are green.
3. Check to see that the DSL LED is green
4. Check the settings on your PC. Again, refer to the easy start guide for more details
5. Check the Wireless Gateway's settings.
6. From your PC, can you PING the Wireless Gateway? Assuming that the Wireless Gateway has DHCP enabled and your PC is on the same subnet as the gateway, you should be able to PING the gateway.
7. Can you PING the WAN IP? Your ISP should have provided the IP address of their server. If you can ping the Wireless Gateway and your protocols are configured correctly, you should be able to ping the ISPs network. If you cannot PING the ISPs network, make sure you are using the correct protocols with the correct VPI/VCI values.
8. Make sure NAT is enabled for your connection. If NAT is disabled the Wireless Gateway will not route frames correctly (except in Bridge connection).

6.2 I can't connect to the Wireless Gateway.

1. Check to see that the power LED is green and that the network cables are installed correctly; see the easy start guide for more details.
2. Make sure that your PC and the Wireless Gateway is on the same network segment. The Wireless Gateway's default IP address is 192.168.1.1. If you are running a Windows based PC, you can open a DOS window and type IPCONFIG; make sure that the network adapter that is connected to the gateway is within the same 192.168.1.x subnet.
3. Also, your PC's Subnet Mask should match the gateways subnet mask. The gateway has a default subnet mask of 255.255.255.0.
4. If this still does not work, press the reset button for 10 seconds. This will place the gateway into its factory default state. Go through the above procedures again.
5. Make sure NAT is enabled for your connection. If NAT is disabled the Wireless Gateway will not route frames correctly (except in Bridge connection).

6.3 The DSL Link LED continues to blink but does not go solid

1. This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.
2. Verify that the phone line is connected directly to the wall and to the line input on the Wireless Gateway.
3. Make sure that for every parallel phone line connected to telephone or fax to install with a micro filter.

6.4 The DSL Link LED is always off

1. Make sure you have DSL service. You should get some kind of information from your ISP that states that DSL service is installed. You can usually tell if the service is installed by listening to the phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. Verify that the phone line is connected directly to the wall and to the line input on the Wireless Gateway. If the phone line is connected to the phone side of the Wireless Gateway or you have a splitter installed on the phone line, the DSL light will not come on.

7. Wireless Gateway terms

What is DSL ?

DSL which is short for Digital Subscriber Line is a technology that increases the digital capacity of a ordinary telephone line into home or office and , because it is utilizing the unused bandwidth, the line allows normal phone usage and signal to be for broadband to be used at the same time. DSL has the capability to impart "always-connected" services, thus eliminating the need to dial in to the service

What is a firewall?

A firewall is protection between the Internet and your local network. It acts similarly to the firewall in your car, protecting the interior of the car from the engine. Your car's firewall has very small opening that allow desired connections from the engine into the cabin (gas pedal connection, etc), but if something happens to your engine, you are protected.

The firewall in the Wireless Gateway is very similar. Only the desired connections that you allow are passed through the firewall. These connections are normally originating from the local network; such as web browsing, checking your email, downloading a file, and playing a game. However, in some cases, you can allow incoming connections so that you can run programs like a web server.

What is NAT?

NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address for you to access the Internet through. However, you may have several machines on your local network that want to access the Internet at the same time. The Wireless Gateway provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine.

Occasionally, there are certain programs that don't work well through NAT. Some games, and some specialty applications have a bit of trouble. The Wireless Gateway contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a SERVER though. When running a server, please see the DMZ section below.

What is a DMZ?

DMZ really stands for Demilitarized Zone. It is a way of separating out part of your local network so that is more open to the Internet. Suppose that you want to run a web-server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to "isolate" the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.

Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the servers network address to others, you must provide the address of the Wireless Gateway. The Wireless Gateway "fakes" the connection to your machine.

You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers, etc) should NOT be connected to the DMZ

What is a Gateway?

The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers or gateways are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.

What is SSID ?

A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network ([WLAN](#)). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area

What is WEP ?

Wired Equivalent Privacy (WEP) is a security protocol, specified in the [IEEE](#) Wireless Fidelity ([Wi-Fi](#)) standard, [802.11b](#), that is designed to provide a wireless local area network ([WLAN](#)) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network ([LAN](#)) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data [encryption](#) protects the vulnerable wireless link between [clients](#) and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks ([VPNs](#)), and [authentication](#) can be put in place to ensure privacy.



Lynx: constellation introduced by J. Hevelius in 1687. The Lynx is a nocturnal wildcat with superb eyesight. The observers of this constellation would have to be “lynx-eyed” to see it.



© 2005 Starbridge Networks LLC. All rights reserved.

www.starbridgenetworks.com